Encryptiebeleid Sabewa Zeeland

11-04-2023

Mirjam van Delft – Kaijser
Informatieadviseur a.i.

Versiebeheer

Versie	Datum	Door	Wijzigingen
0.1	10-3-2023	Mirjam van Delft - Kaijser	
1.0	28-11-2023	Mirjam van Delft – Kaijser	Vastgesteld door MT

1.1 Relatie met overige documenten

- Baseline Informatiebeveiliging Overheid (BIO)
- Strategisch Informatiebeveiligingsbeleid Sabewa Zeeland 2023 - 2027

1.2 Verwijzingen naar de Baseline Informatiebeveiliging voor de Overheid (BIO)

10.1.1 Beleid inzake gebruik van cryptografische beheersmaatregelen

2. Inleiding

Het is van grootbelang dat wij de vertrouwelijkheid, integriteit en beschikbaarheid van onze data waarborgen. Daarom moet data met de classificatie Basis BeveiligingsNiveau (BBN) 2 of hoger beschermd worden met cryptografische maatregelen.

De beleidsuitgangspunten in dit encryptiebeleid zijn ontleend aan de Baseline Informatiebeveiliging Overheid (BIO). Bij elk beleidsuitgangspunt zijn de bijbehorende doelstelling en het kader uit de BIO opgenomen. Hierin zijn opgenomen:

- Control
  Dit is het nummer van de in die BIO beschreven control die voor dit onderwerp van toepassing is. Dit kan een Controle nummer zijn. overeenkomstig met ISO 27002 (blauwe tekst), of een O-maatregelnummer[1] (groene tekst). Op basis van een risicoafweging wordt door het management bepaald hoe moet worden voldaan aan de gestelde beveiligingsdoelstellingen van de controls. Voor het voldoen aan deze doelstellingen kunnen implementatierichtlijnen uit de ISO 27002, overheidsmaatregelen en/of operationaliseringen in handreikingen worden gebruikt.
- BNN – Basisbeveiligingsniveau.
  De BIO onderscheidt drie niveaus:
  - Voor BBN1 ligt de nadruk op 'wat mag minimaal verwacht worden?'.
  - Voor BBN2 ligt de nadruk op de bescherming van de meest voorkomende categorieën informatie volgens het principe 'valt de maatregel onder goed huisvaderschap; toont deze beveiliging de betrouwbare overheid?'
  - BBN3 is van toepassing op gerubriceerde informatie Departementaal Vertrouwelijk dan wel vergelijkbaar vertrouwelijk bij andere overheidslagen, waarbij weerstand tegen statelijke actoren of vergelijkbare dreigers nodig is.
- Verantwoordelijke
  In het algemeen geldt dat onderdelen van de BIO op verschillende plaatsen in de organisatie worden toegepast op grond van verschillende verantwoordelijkheden en gezagsverhoudingen. De BIO onderscheidt drie (hoofd)rollen:
  - Secretaris/algemeen directeur
    Als eindverantwoordelijke voor het beveiligingsbeleid in de organisatie is de secretaris/algemeen directeur verantwoordelijk voor de uitvoering van organisatiebrede vraagstukken ten aanzien van informatiebeveiliging.
  - Proceseigenaar
    Onder de proceseigenaar wordt de lijnmanager verstaan die verantwoordelijk is voor de beveiliging van het betreffende proces / informatiesysteem.
  - Dienstenleverancier
    Bedoeld wordt de dienstenleverancier (bijvoorbeeld SSO) binnen de overheid of organisaties in de markt waaraan de secretaris/algemeen directeur of proceseigenaar (een deel van) de beveiligingstaak inbesteedt respectievelijk uitbesteedt.

[1] *O-maatregel is de overheidsmaatregel gebaseerd op een ISO 27002 control*

3. Cryptografie

Doelstelling: Zorgen voor correct en doeltreffend gebruik van cryptografie om de vertrouwelijkheid, authenticiteit en/of integriteit van informatie te beschermen.

Control	BNN	Gedrag / procedure	Verantwoordelijke
10.1.1	2	**Beleid inzake het gebruik van cryptografische beheersmaatregelen** Ter bescherming van informatie behoort een beleid voor het gebruik vancryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.	Directeur (intern)
10.1.1.1	2	In het cryptografiebeleid zijn minimaal de volgende onderwerpen uitgewerkt: (a) Wanneer cryptografie ingezet wordt. (b) Wie verantwoordelijk is voor de implementatie. (c) Wie verantwoordelijk is voor het sleutelbeheer. (d) Welke normen als basis dienen voor cryptografie en de wijze waarop de normen van het Forum worden toegepast. (e) De wijze waarop het beschermingsniveau vastgesteld wordt. (f) Bij communicatie tussen organisaties wordt het beleid onderling vastgesteld.	
10.1.1.2	2	Cryptografische toepassingen voldoen aan passende standaarden.	

1. Data met de classificatie BBN2 of hoger wordt beschermd door cryptografische maatregelen. Hiermee wordt de vertrouwelijkheid van de data beschermd en ongeautoriseerde toegang voorkomen. Daarnaast wordt cryptografie gebruikt om de integriteit van de informatie te garanderen en om te verifiëren dat de informatie afkomstig is van een betrouwbare bron.
2. De verantwoordelijkheid van de implementatie van de cryptografie ligt bij de CISO of de IT-beheerder. Zij zorgen ervoor dat de juiste cryptografische maatregelen worden genomen.
3. Het sleutelbeheer wordt zoveel mogelijk door de leveranciers van Cloud software zelf uitgevoerd. Daarnaast wordt sleutelbeheer belegd bij de Functioneel- of IT beheerder. De sleutelbeheerder is verantwoordelijk voor het (laten) genereren, distribueren en beheren van de sleutels die nodig zijn voor het ver- en ontsleutelen van de data. Er moeten voldoende controlemechanismen zijn om te voorkomen dat sleutels niet verloren gaan of in verkeerde handen vallen.
4. Gegevenstransport wordt naar de laatste stand der techniek beveiligd met cryptografie (conform Forum Standaardisatie). Opgeslagen gegevens in een clouddienst worden naar de laatste stand der techniek beveiligd met encryptie en met een tenminste voor het doel toereikende sleutellengte.
5. Het beschermingsniveau wordt vastgesteld op basis van de classificatie van de data. Hiervoor worden de handreikingen uit de BIO gebruikt. Data met classificatie BBN 2 of hoger moet beschermd worden met cryptografische maatregelen. Het beschermingsniveau kan ook afhankelijk zijn van andere factoren, zoals de gevoeligheid van de data en de mogelijke impact van een datalek.

6. Bij communicatie tussen organisaties moeten beide partijen overeenstemming bereiken over het gebruik van cryptografie. Het beleid van beide partijen moet worden vastgesteld om ervoor te zorgen dat de bescherming van data gewaarborgd blijft. Het is belangrijk dat het beleid van beide partijen aansluit bij de normen van de BIO en het Forum Standaardisatie. Beide partijen bepalen het benodigde beschermingsniveau door het classificeren van de betreffende data.

4. Rapportage en controle

- Het management controleert minimaal eens per kwartaal of het encryptiebeleid wordt uitgevoerd voor de informatiesystemen waar zij verantwoordelijk voor zijn.

Aldus vastgesteld door het MT van Sabewa Zeeland op *28-11-2023*

Aldus vastgesteld door het Dagelijks Bestuur van Sabewa Zeeland op *[datum]*